Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 1 1 **********AUTO**ALL FOR AADC 300
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

August 3, 2023

NOTICE OF DATA BREACH

Dear Sample A. Sample:

I am writing on behalf of Unum Group ("Unum") and its subsidiaries, including Starmount Life Insurance Company, to notify you that we recently experienced a cybersecurity incident resulting from a security vulnerability in a third-party software application used by Unum. Unum provides you with benefits, such as dental or vision coverage. The application involved is MOVEit Transfer, a file transfer application made available by Progress Software Corporation ("Progress") that Unum and many other organizations in the U.S. and globally used to handle certain data transfers. As detailed in a June 7, 2023 U.S. government advisory, there has been widespread exploitation of a security vulnerability in MOVEit Transfer, which has reportedly impacted hundreds of organizations. We are taking this matter very seriously and providing this letter to help you understand what happened and what we are doing in response.

What Happened? On June 1, 2023, Unum detected suspicious activity involving an instance of its MOVEit Transfer application. Unum promptly launched an investigation with the assistance of third-party cybersecurity experts. On June 4, 2023, the investigation identified evidence that, between May 31, 2023 and June 1, 2023, an unauthorized party had exploited the security vulnerability to copy data. On July 22, 2023, Unum learned that records containing your personal information were impacted.

What Information Was Involved? The information involved varied by individual and may have included name, date of birth, address, Social Security number or individual tax identification number, medical information, health insurance claim information, and policy information. Financial information and other government issued identification numbers were involved for a limited number of individuals.

What We Are Doing. Upon learning of this issue, Unum took several steps to respond, including taking MOVEit Transfer offline, implementing vendor-recommended actions including application of patches as Progress made them available, notifying law enforcement, and monitoring publicly available information regarding this vulnerability. Although this incident did not affect Unum systems directly beyond the impacted instance of MOVEit Transfer, Unum continues to further enhance its security controls to protect from cyber threats. We also have arranged for you to obtain, at no cost to you, 24 months of credit monitoring services from Experian. Information regarding these services is included in Attachment 1 to this letter.

What You Can Do. We encourage you to sign up for the free credit monitoring and other services from Experian. Information about enrollment is included in Attachment 1 to this letter. We also recommend that you remain vigilant by reviewing your account statements and monitoring your free credit reports for signs of suspicious activity. Please find additional information in Attachment 2 to this letter.

For More Information. We regret that this incident occurred. If you have questions or concerns regarding this matter, please contact (833) 309-0979 toll-free, Monday through Friday 8:00 a.m. to 10:00 p.m. Central or Saturday and Sunday 10:00 a.m. to 7:00 p.m. Central (excluding major U.S. holidays). Please be prepared to provide your engagement number [redacted].

Sincerely,

Ciera Carter

Ciera Carter
Assistant Vice President
Customer Contact Centers

Attachment 1: Credit Monitoring Services Enrollment Information

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by November 3, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/RR3Bplus
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-309-0979 by November 3, 2023. Be prepared to provide engagement number B096435 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE[TM]:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet:** Provides assistance with canceling/replacing lost or stolen credit, debit, and medical cards.
- **Child Monitoring:** For 10 children up to 18 years old, Internet Surveillance and monitoring to determine whether enrolled minors in your household have an Experian credit report are available. Also included are Identity Restoration and up to $1M Identity Theft Insurance**.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Attachment 2: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information
Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Whether or not you enroll in the credit monitoring product offered, you also have the right to place an initial fraud alert on your file at no cost. An initial fraud alert lasts one (1) year and is placed on a consumer's credit file. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Fraud alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A fraud alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies. You may also contact any of the consumer reporting agencies or the FTC for more information regarding fraud alerts. The contact information for the three nationwide credit reporting agencies is:

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
https://www.experian.com/help/

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
https://www.transunion.com/credit-help

Free Credit Report Information
You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. We encourage you to review your rights pursuant to the FCRA by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also

should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself and prevent such activity. If you are a resident of the District of Columbia, Iowa, Maryland, New York, North Carolina, or Oregon, you can also reach out to your respective state's Attorney General's office at the contact information below. Residents of all other states can find information on how to contact your state attorney general at https://www.naag.org/ find-my-ag/.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357) / www.ftc.gov/idtheft

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392 / https://justice.oregon.gov

New York Attorney General's Office
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/consumer-frauds-bureau/identity-theft

North Carolina Department of Justice
114 West Edenton Street
Raleigh, NC 27603
1-919-716-6400
https://ncdoj.gov/protecting-consumers/identity-theft/

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, DC 20001
1-202-727-3400 / oag.dc.gov

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 /
www.marylandattorneygeneral.gov

Consumer Protection Division
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926 / www.iowaattorneygeneral.gov

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
https://riag.ri.gov/

Security Freeze Information
You have the right to request a free security freeze (aka "credit freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a credit freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A credit freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding security freezes.

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
http://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
https://www.transunion.com/credit-freeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Monitor Your Personal Health Information
If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline.